مواقع اختصار الروابط والمخاطر الأمنية

الكاتب : عبدالكريم العنزي (Ghost Hacker)
المدونة : http://gh05th4ck.wordpress.com



مقدمة:

بعض الروابط (URL) تكون مكونه من حروف كثيرة مثلا رابط لمقالة في مركز التميز لأمن المعلومات
http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/45-wireless-security/1152-wireless-securityy.html
حجم الرابط كبير جداً مما يعني صعوبة في عملية كتابته و تبادله مع الأصدقاء.
بعد عملية اختصار الرابط من خلال أحد مواقع الاختصار (URL Shortener) يصبح بهذا الشكل
http://bit.ly/cHmYwi
عند الدخول على الرابط القصير هذا سيقوم بدوره بتحويلك إلى الرابط المختصر طويل الحجم.
ظهرت خدمات أو مواقع اختصار الروابط لتحل مشكلة طول الـ URL حيث يمكن من خلالها تقصير رابط مكون من ٥٠ حرف إلى رابط مكون من ١٠ حروف.
أستخدم الموقع الاجتماعي الشهير Twitter هذه التقنية لتوفير عدد أحرف أكثر في صندوق الكتابة
حيث أن صندوق الكتابة بالأصل لا يقبل سوى ١٠٠ حرف، فإذا أضاف المستخدم كتابة تحتوى على رابط مكون من ٩٠ لن يتبق له سوى ١٠ حروف ليكتب لمحة عن محتوى الرابط وهذا غير كاف أبداً.

المخاطر الأمنية:

قد تستخدم تقنية (URL Shortener) لتضليل الروابط الخبيثة التي تحتوى على مواد ضارة أو شيفرات خبيثة .
حيث سيتم اختصارها لكسب ثقة الضحية وإيهامه أن الرابط المختصر يحتوى على خبر هام في جريدة مثلا :).
لذلك ليعلم الجميع أن الدخول على أي موقع من خلال الـ URL الخاص به
لا يعني أن نفس محتوى الموقع المطلوب سيظهر لك، قد تحتوى صفحة الموقع الذي تم طلبه على شيفرة تحويل تقوم بعملية إرسالك بشكل تلقائي إلى URL أخرى الذي بدوره قد يحتوى على مادة ضارة قد تضر بنظامك أو تنتهك خصوصيتك.

كيفية الوقاية:

- بالبداية يجب عليك تأمين المتصفح الخاص بك لأن المهاجم ليقوم بوضع شيفراته الخبيثة يجب أن تتوفر لديه ثغره أمنية في المتصفح نفسه لذلك
يجب عليك تحديث المتصفح إلى أخر إصدار كما يجب التماس التحديثات والرقع الأمنية.
- قم بتعطيل الجافا سكربت في المتصفح وتفعيلها للمواقع الموثوقة فقط.
- تجنب فتح الروابط الغير موثوق بها.
- استخدم موقع untiny.me / Untiny الذي يقوم بعملية عكسية لمواقع اختصار الروابط ويسترجع الرابط المختصر.



صورة تبين عملية استرجاع رابط مختصر في Untiny

أنتهى ..